National Security Agency/Central Support Service

INFORMATION
ASSURANCE
DIRECTORATE

Introduction to the Community Gold Standard

Version 1.1.1

The Community Gold Standard (CGS) for information assurance (IA) provides comprehensive, measurable, IA guidance for securing NSS Enterprises while enabling the mission in the face of continuous attack. CGS defines what it means for Capabilities to be considered “gold.” That is, it characterizes the highest level of practice for IA Capabilities in accordance with policies, standards, and best practices, while considering the limitations set forth by current technologies and other constraints.

07/30/2012

Introduction to the Community Gold Standard

Version 1.1.1

Table of Contents

1 Revisions

Name	Date	Reason	Version
CGS Team	30 June 2011	Initial release	1.1
CGS Team	30 July 2012	Inclusion of new IAD document template & Synopsis	1.1.1

2 Background

The Community Gold Standard (CGS) is comprehensive guidance for the National Security Systems (NSS) community. The NSS, as defined by National Security Directive 42, “National Policy for the Security of National Security Telecommunications and Information Systems,” include those telecommunications and information systems operated by the U.S. Government, its contractors, or agents, that contain classified information or, as set forth in United States Code, Title 10, Section 2315[1] “that involve intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapon system, or equipment that is critical to the direct fulfillment of military or intelligence missions.”

3 Purpose

The CGS for IA provides comprehensive, measurable, IA guidance for securing NSS Enterprises while enabling the mission in the face of continuous attack. CGS defines what it means for Capabilities to be considered “gold.” That is, it characterizes the highest level of practice for IA Capabilities in accordance with policies, standards, and best practices, while considering the limitations set forth by current technologies and other constraints.

The CGS does not require each agency or organization Enterprise to achieve the Gold Standard level of practice for every Capability. In fact, achieving gold for some Capabilities may be impractical or cost prohibitive. It does intend, however, that each Enterprise review the Gold Standard guidance and decide to what level implementation of the guidance provided is appropriate for its Enterprise based on mission needs, threat, current security posture, and resources.

4 Evolution

CGS began as a challenge from DIRNSA to capture best practices in IA while protecting NSS Enterprises. The CGS Framework and Capabilities were developed internally by NSA experts and have been thoroughly vetted through NSS Community reviews. The CGS will continually evolve as technology evolves and policy changes. Updates to the

[1] 10 U.S.C. § 2315. “Law inapplicable to the procurement of automatic data processing equipment and services for certain defense purposes.”

CGS will be captured and used to drive policy changes, define research agendas, and initiate industry participation.

5 CGS Organization

This section describes the CGS Framework, Capability Areas, and individual Capability structure. The Capability structure includes a definition; Gold Standard guidance; environment pre-conditions; Capability post-conditions; organizational implementation considerations; Capability interrelationships; related security controls; directives, policies, and standards; cost considerations; and guidance statements. Each of these areas is further described within this section.

5.1 Framework

The CGS Framework encompasses 11 Overarching Capability Areas and defines the set of IA Capabilities necessary to provide full-spectrum protection and defense for NSS Enterprises. The Capability Areas contain guidance for a comprehensive, enterprise-wide, IA solution, including Enterprise Operations, Governance (business processes), and Corporate Culture. The guidance associated with each of the Capabilities provides a holistic view of IA for the Enterprise and is intended to help the NSS Community understand and rapidly respond to threats, provide a layered defense, and make informed risk decisions. The Framework and corresponding guidance provide organizations with recommended, comprehensive, IA components to assist in identifying specific gaps in Enterprise protection and in prioritizing the implementation of future IA projects and programs based on mission, current security posture, threats, and resource considerations.

Chief Information Security Officers and Chief Information Officers, as well as other decision-makers on programs or projects, use the CGS Framework, shown in Figure 1, as a basis for deciding the extent to which each Capability is required for the Enterprise. The CGS Capability descriptions help the decision-makers define and prioritize IA integration into programs and projects.

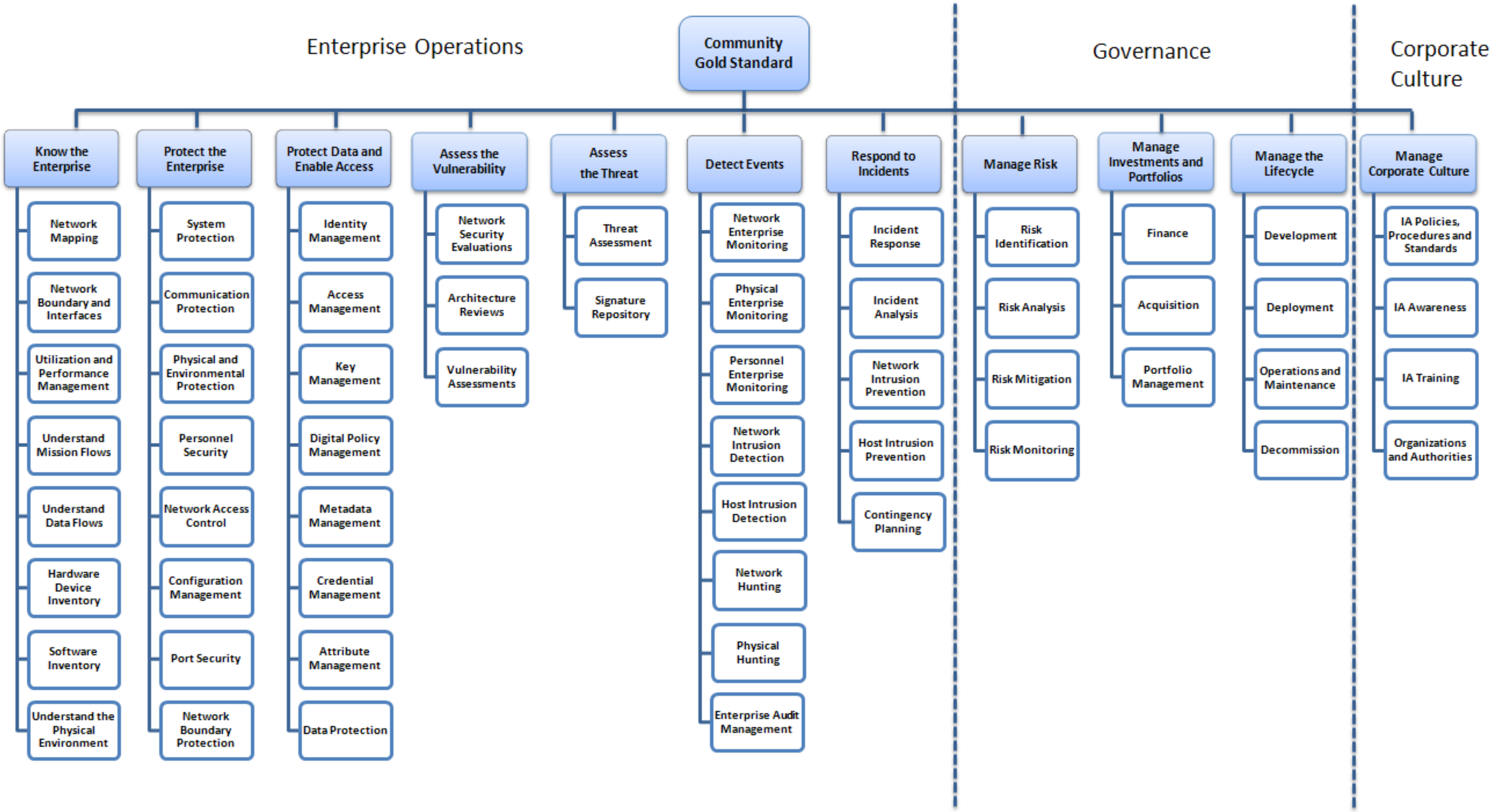

Figure 1. Community Gold Standard Framework

5.2 Capability Areas

The Capability Areas, as indicated by the 11 higher-level boxes in Figure 1, are structured to place complementary Capabilities together to achieve a single IA goal. Each of the Capabilities in an area accomplishes its individual objective while contributing to the overall purpose of the Capability Area.

5.2.1 Know the Enterprise

The Know the Enterprise Capability Area provides the Enterprise with the Capabilities necessary to visualize the network and understand the relationships and connectivity among all devices and their communication, including understanding the interfaces to and interdependencies with other networks and ensuring availability and reliability of resources. It provides the foundational knowledge of the people, facilities, and environmental factors in the Enterprise. It maps the interactions between people, processes, technology, and the environment; identifies the source, destination, and path of all data; and identifies and tracks hardware and software assets.

5.2.2 Protect the Enterprise

The Protect the Enterprise Capability Area provides the Enterprise with the Capabilities necessary to protect the network, its boundaries, and both systems and communications. It provides the ability to screen personnel who may need access to the Enterprise and its resources and prevent unauthorized access to facilities, systems, resources, or information. It establishes and maintains integrity of products and systems through configuration control and ensures that only authorized personnel or systems gain access to and uses Enterprise resources.

5.2.3 Protect Data and Enable Access

The Protect Data and Enable Access Capability Area provides the Enterprise with the Capabilities necessary to protect data in use, at rest, and in transit. It enforces the permissions that define the actions that an entity may or may not perform against a resource; provides, controls, and maintains the cryptographic keys, key material, and key products required to support operational missions; and generates, validates, and maintains IA metadata and metadata schemas. It manages the properties associated with entities in the Enterprise; manages the creation, issuance, maintenance, revocation, and status of identity credentials; and associates identifiers with entities that can perform an action anywhere in the Enterprise. Finally, it generates converts, manages conflicts, validates, provisions, and executes machine-readable policies that enforce the management, use, and protection of Enterprise resources.

5.2.4 Assess the Vulnerability

The Assess the Vulnerability Capability Area provides the Enterprise with the Capabilities necessary to identify potential weaknesses across all susceptible areas. It includes assessment of vulnerabilities in physical, personnel, technological, and environmental protections.

5.2.5 Assess the Threat

The Assess the Threat Capability Area provides the Enterprise with the Capabilities necessary to identify, analyze, and prioritize threat information. Assess the Threat uses data captured by other Capabilities to identify threats and threat sources, understand a threat source's abilities, and determine the probability of the threat exploiting a known vulnerability.

5.2.6 Detect Events

The Detect Events Capability Area provides the Enterprise with the Capabilities necessary to monitor and detect anomalies within the Enterprise systems and the physical infrastructure in order to detect malicious activity. It proactively looks for indicators of an active threat or exploitation of vulnerabilities, provides active and passive monitoring of the Enterprise to share awareness of event changes, and monitors physical and environmental controls to prevent unauthorized physical access to facilities and systems. It also provides assurance that the personnel granted access to facilities, systems, and information have current authorization and clearances. Detect Events identifies, collects, correlates, analyzes, stores, and reports audit information.

5.2.7 Respond to Incidents

The Respond to Incidents Capability Area provides the Enterprise with the Capabilities necessary to establish policy, procedures, and technical measures designed to maintain or restore operations should an incident occur. It enables the Enterprise to prevent host-based and network-based system attacks and provides first line of protection against anomalous activity by responding to signature-based and statistical pattern-based alerts and notifications. It is responsible for analyzing and responding to incidents including triage, escalation, isolation, and restoration of Enterprise functions during and after technical, personnel, physical, and environmental incidents, and for developing, recommending, and coordinating Enterprise mitigation actions provided by the Risk Mitigation Capability.

5.2.8 Manage Risk

The Manage Risk Capability Area provides the Enterprise with the Capabilities necessary to collect and analyze risk-related data. It establishes a relationship between threat and vulnerability pairs, determines whether these pairs have influence on the Enterprise's risk, decides which mitigations will be applied to the risks, and implements those mitigations. It also assesses the effectiveness of the risk decisions and monitors the current security posture, determining if there are any gaps.

5.2.9 Manage Investments and Portfolios

The Manage Investments and Portfolios Capability Area provides the Enterprise with the Capabilities necessary to understand and effectively budget for the Enterprise's IA resources. It ensures proper planning for and allocation of IA resources, including consideration of technical, personnel, physical, and environmental IA needs. It also ensures the Enterprise follows secure acquisition processes and obtains IA products and services from authorized providers.

5.2.10 Manage the Lifecycle

The Manage the Lifecycle Capability Area provides the Enterprise with the Capabilities necessary to ensure that IA is incorporated throughout the development lifecycle. The Capabilities within Manage the Lifecycle make certain that the necessary security personnel, decision-makers, and stakeholders are included throughout the process to ensure the security requirements are properly defined, approved, tested, and implemented.

5.2.11 Manage Corporate Culture

The Manage Corporate Culture Capability Area provides the Enterprise with the Capabilities necessary to identify, establish, and manage the IA policies, procedures, and standards needed at all levels of the Enterprise to ensure the IA vision and goals can be met. In addition, it establishes the authorities and organizations within the Enterprise responsible for making IA decisions. It defines and manages the training and awareness programs necessary to ensure understanding of the Enterprise IA goals and details proper execution of the IA processes and procedures.

5.3 Composition of the Capability Documents

Each Capability document consists of the following sections. These sections provide an introduction to the content in each document. Within the Capability documents, these sections will be defined within the limitations of current technologies.

5.3.1 Capability Definition

The Definition section of each capability write-up provides a high-level introduction to the Capability. It aids the reader in understanding why the Capability is important to the

Enterprise. It also defines the different parts of the Capability and assists in understanding how the Capability will function within the Enterprise.

5.3.2 Capability Gold Standard Guidance

The Capability Gold Standard Guidance evaluates the Enterprise needs and overlays the expected Gold Standard behavior. The guidance goes beyond the concept of "good enough" when describing the Gold Standard recommendations, considers industry best practices, and describes a level of security that not only meets current standards but also exceeds them across the Enterprise.

5.3.3 Environment Pre-Conditions

The Environment pre-conditions provide insight into environmental, user, and technological aspects needed for Capability implementation. These pre-conditions are services or other Capabilities that must be in place within the Enterprise for the Capability to function.

5.3.4 Capability Post-Conditions

The Capability post-conditions define what the Capability will provide. They define functions that the Capability will perform or constraints that the Capability will operate under when performing its function.

5.3.5 Organizational Implementation Considerations

Organizational implementation considerations provide insight into what the organization needs to establish, ensure, and have in place for the specified Capability to be effective. It provides guidance specific to the actions, people, processes, and departments that an organization will need to execute or establish to implement the Capability.

5.3.6 Capability Interrelationships

Capability interrelationship maps the Capability within the document to other Capabilities that it either relies on or that rely on it for information, data, monitoring, policies, procedures, standards, alerts, or other functions. Although there are many relationships between the Capabilities, the focus is on the primary relationships in which the Capabilities directly communicate or influence one another. In many cases there are secondary relationships (not indicated in the mapping), which are provided as a result of the primary relationships.

5.3.6.1 Required Interrelationships

The Required Interrelationships section provides the other Capabilities within the Community Gold Standard framework that are necessary for each Capability to operate.

5.3.6.2 Supporting Interrelationships

The Supporting Interrelationships section provides the other Capabilities within the Community Gold Standard framework that are not necessary for each Capability to operate, although they support the operation of the Capability.

5.3.7 Security Controls

The Security Controls section provides a mapping of each Capability to the appropriate controls. Initially, the mapping will include controls from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. The controls and their enhancements are granularly mapped according to their applicability to each Capability. In some instances, a control may map to multiple Capabilities. The Capability documents are not responsible for providing guidance on implementation of the security controls.

Organizations will be responsible for selecting appropriate security controls, implementing the controls correctly, and demonstrating the effectiveness of the controls in satisfying their stated security requirements. Organizations will be responsible for implementation in accordance with the appropriate Committee on National Security Systems (CNSS), NIST, Department of Defense (DoD), Intelligence Community (IC), or federal/civil policy. In determining which security controls apply to the organization, SP 800-53 and CNSS 1253 can be effectively used to determine applicability and potential impact levels as they potentially affect loss of confidentiality, integrity, or availability within the Enterprise.

The CGS security control mapping does not contain any supplemental guidance or mappings between controls, which are provided in SP 800-53. The implementer should refer to the SP 800-53 for any supplemental guidance and references. They can be found easily by referring to the mapped controls.

5.3.8 Directives, Policies, and Standards

The Directives, Policies, and Standards section identifies existing policies and directives applicable to the Capability. The information provided in this section contributes to the Capability's Gold Standard Guidance, along with other applicable areas. The documents referenced in this section are not agency specific and therefore do not include any directives, policies, or standards that are applicable to only one agency.

5.3.9 Cost Considerations

Although the CGS does not address cost when defining each Capability, it is recommended that the Enterprise consider cost when deciding which Capabilities to implement and to what extent to implement them. In addition to the implementation of the CGS Capabilities, costs associated with related requirements should be considered, including support, documentation, procedures, training, peripherals, communications, and maintenance. Upfront costs as well as ongoing operational, upgrade, and maintenance costs should also be considered. Each Enterprise likely operates in an environment that is unique in its own way. A lot of operating environments will share many similar characteristics, but they will not all have an identical threat level, use identical technologies, and be supported by identical resources. Each Enterprise will adopt CGS Capabilities appropriately in accordance with their mission, operational, and environmental needs based on the resources they have available. Those Enterprises that operate in a high-threat environment will likely want to implement more Capabilities than Enterprises that operate in comparatively low-threat environments.

Cost considerations are factors that involve a tradeoff of limited resources while trying to achieve an objective. Cost considerations also encompass more than just monetary resources. Costs can include all manner of factors including money, time, risk, and opportunity costs. These are factors the Enterprise should consider when they are evaluating the various implementation options for each Capability. Most of the Capabilities share several common cost considerations. In addition, most Capabilities also have some cost considerations that are less common or are completely unique. The Enterprise implementing the CGS will need to consider the cost considerations associated with each Capability in order to estimate the total cost of implementation to effectively evaluate which Capabilities to adopt and how to implement them.

5.3.10 Guidance Statements

The Guidance Statements are intended to provide an Organization with a list of standalone statements that are representative of the narrative guidance provided in Section 3 (Capability Gold Standard Guidance) of each of the CGS Capability documents.